2018R01347/DS

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
	:	Crim. No. 19-
v.	:	
	:	18 U.S.C. § 371
ARTEM RADCHENKO and	:	18 U.S.C. § 1030
OLEKSANDR IEREMENKO	:	18 U.S.C. § 1343
	:	18 U.S.C. § 1349
	:	18 U.S.C. § 2

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

Count One
(Conspiracy to Commit Securities Fraud)

Overview

1. From in or about February 2016 through in or about March 2017, the defendants and others conspired to enrich themselves through a sophisticated securities fraud scheme that involved hacking into the computer networks of the United States Securities and Exchange Commission ("SEC") and stealing annual, quarterly and current reports of publicly traded companies before the reports were disseminated to the investing public. Many of the stolen reports contained material non-public information concerning, among other things, the earnings of the companies. The defendants and others sought to profit illegally from their scheme by selling access to the material non-public information contained in these as-yet undisclosed reports

and by trading in the securities of the companies before the investing public learned the information.

Relevant Individuals and Entities

2. At all times relevant to this Indictment:

a. Defendant ARTEM RADCHENKO ("RADCHENKO") resided in Ukraine.

b. Defendant OLEKSANDR IEREMENKO ("IEREMENKO") was a computer hacker who was a Ukrainian national. From 2010 to 2015, IEREMENKO engaged in a scheme to hack certain newswire services that edit and disseminate press releases for publicly traded companies (the "Newswire Hacking Scheme"). In carrying out the scheme charged herein, IEREMENKO employed some of the same techniques and methods that he had used in the Newswire Hacking Scheme.

c. Co-conspirator 1 ("CC-1") resided in Ukraine.

d. The New York Stock Exchange ("NYSE") was the largest stock exchange in the United States based on market capitalization. The NYSE's trade processing and data services were performed at its data center in or around Mahwah, New Jersey.

e. The NASDAQ Stock Market ("NASDAQ") was the second largest stock exchange in the United States based on market capitalization. The NASDAQ did not have a central trading floor. Instead, it relied on computer servers to facilitate all trading activity. The NASDAQ maintained computer servers in or around Carteret, New Jersey.

f. Companies whose shares were registered with the SEC and traded on the NASDAQ or the NYSE were subject to ongoing disclosure requirements designed to keep investors informed about material changes in their financial condition and operations. As a result, such public companies filed annual and quarterly reports with the SEC on Forms 10-K and 10-Q, respectively, as well as current reports filed on Form 8-K ("Required Filings"). These Required Filings contained detailed information about, among other things, the financial condition and operations of the companies, including their earnings. This information was treated as highly confidential business information prior to its release to the public. In fact, publicly traded companies making Required Filings were subject to SEC Regulation Fair Disclosure, prohibiting them from making selective disclosures of such material non-public information before disclosing the information to the public generally.

g. The SEC was an agency of the United States government whose duties included maintaining fair, orderly, and efficient markets. The SEC operated the Electronic Data Gathering, Analysis and Retrieval system, known as "EDGAR." The EDGAR computer servers relevant to this Indictment were located in New Jersey.

h. EDGAR was used by public companies to electronically file Required Filings. EDGAR also allowed companies to make test filings hours or days in advance of the public release of the Required Filings ("Test Filings"). Test Filings often contained information that was the same or substantially

similar to the material information that was eventually released to the public in the Required Filings, and, as a result, at the time the Test Filings were made, they often contained material non-public information.

Relevant Terms

3. At all times relevant to this Indictment:

a. A "user agent string" was information sent to a computer accessed by a web browser which identified the version of the web browser being used and the operating system of the computer.

b. An "IP address" was a series of numbers assigned to a particular internet connection. Computers attached to the Internet used an internet connection which was assigned an IP address so that Internet traffic sent from and directed to that computer could be directed properly from its source to its destination.

c. A "directory traversal attack" was a method of gaining unauthorized access to a restricted area of a web server.

d. "Malware" was malicious computer software intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to that person.

e. A "phishing attack" was a fraudulent attempt to obtain sensitive information such as usernames and passwords and/or to install malware by posing as a trustworthy entity in an electronic communication.

f. "Bitcoin" was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin was not issued by any government, bank, or company, but rather was generated and controlled through computer software operating via a decentralized, peer-to-peer network.

g. "Bitcoin addresses" were the particular virtual locations to which Bitcoin were sent and received. A Bitcoin address was analogous to a bank account number and was represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address was controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key could authorize a transfer of Bitcoin from that address to another Bitcoin address.

The Conspiracy

4. From in or about February 2016 through in or about March 2017, in Middlesex County, in the District of New Jersey and elsewhere, the defendants,

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO,

did willfully and knowingly conspire and agree with each other, CC-1, and others to, directly and indirectly, by the use of means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, use and employ, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section 240.10b-5, by: (i) employing

devices, schemes and artifices to defraud; (ii) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (iii) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, contrary to Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

Goal of the Conspiracy

5. It was the goal of the conspiracy for RADCHENKO, IEREMENKO, CC-1, and others, to unlawfully enrich themselves by: (a) hacking into the computer networks of the SEC through a variety of deceptive techniques; (b) stealing Test Filings containing confidential and economically valuable business information constituting material non-public information; and (c) profiting by selling the material non-public information and trading ahead of its public disclosure.

Manner and Means of the Conspiracy

6. It was part of the conspiracy that the defendants and others gained unauthorized access to the computer networks of the SEC by employing a variety of hacking methods, including directory traversal attacks and phishing attacks. The co-conspirators took steps to conceal and misrepresent their identities to illegally gain access to information on the internal networks of the SEC and to avoid detection.

7. It was further part of the conspiracy that the defendants and others employed phishing attacks to send malicious emails to SEC employees that were made to falsely appear as though they originated from actual SEC employees. As a result of the co-conspirators' phishing attacks, which misrepresented their identities, the co-conspirators successfully infected a number of SEC computers with malware. Once these computers were infected, the co-conspirators used them to probe the SEC's network and to steal information to use in their ongoing efforts to gain unauthorized access to Test Filings.

8. It was further part of the conspiracy that the defendants and others employed some of the same methods that IEREMENKO had used in the Newswire Hacking Scheme. For example, they used an IP address in Romania that IEREMENKO controlled (the "Romanian IP Address") and that had been previously associated with a server IEREMENKO used in the Newswire Hacking Scheme. In addition, the defendants' unauthorized access of the computer networks of the SEC frequently employed the same uncommon user agent string used by IEREMENKO in the Newswire Hacking Scheme.

9. It was further part of the conspiracy that, after gaining unauthorized access to the SEC's computer networks pursuant to the directory traversal attacks, the defendants stole and exfiltrated Test Filings containing confidential business information, including material non-public information, from the SEC's network to servers they controlled, including a server in Lithuania (the "Lithuanian Server"). From in or about May 2016 through in or

about October 2016, the defendants exploited the unauthorized access they had gained to the SEC and the EDGAR system by extracting thousands of Test Filings from the EDGAR servers to the Lithuanian Server.

10. It was further part of the conspiracy that, by employing these deceptive methods to steal Test Filings and extract them from the United States via the Lithuanian Server, the co-conspirators obtained material non-public information of numerous publicly traded companies, with the goal of having other co-conspirators monetize that information through trading.

11. It was further part of the conspiracy that the defendants provided access to the stolen Test Filings to other co-conspirators for the purpose of executing profitable trades in brokerage accounts controlled by these other co-conspirators. The conspiracy was designed for the traders to use the stolen material non-public information to trade before the information was made available to the investing public.

12. It was further part of the conspiracy that RADCHENKO recruited traders to join the conspiracy and maintained notes for himself describing the SEC's role in financial reporting and the co-conspirators' access to the SEC's network. The notes provided in substance and in part as follows:

> SEC is a resource where all quarterly and annual performance reports of U.S. companies are available. SEC regulates the stock market.
>
> Every company is required to report to the SEC its financial results in the form of annual and quarterly reports.

> Every company is required to report important issues, such as bankruptcies or CEO replacements to the SEC.
>
> There is plenty of additional information available, such as database access information, initial codes, networks access, etc.

13. It was further part of the conspiracy that co-conspirators profited by executing trades in the securities of the publicly traded companies prior to the public disclosure of the material non-public information. For example, on or about May 19, 2016, at approximately 3:32 p.m., a Test Filing containing material non-public information relating to Public Company 1's second quarter results was uploaded to the SEC's EDGAR servers. At approximately 3:38 p.m., RADCHENKO, IEREMENKO, and others used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, and steal the Public Company 1 Test Filing that had just been uploaded to EDGAR. Between approximately 3:42 p.m. and 3:59 p.m., a trading account associated with CC-1 (the "CC-1 Trading Account") purchased approximately 121,000 shares of the stock of Public Company 1 for more than approximately $2.4 million. At approximately 4:02 p.m., the material non-public information in the Test Filing was made available to the investing public when Public Company 1 released its second quarter earnings report and announced that it expected to deliver record earnings in the 2016 fiscal year. By the end of the next day, the CC-1 Trading Account had sold the position it acquired the day before for a profit of more than $270,000.

Overt Acts

14. In furtherance of the conspiracy and to effect the unlawful object thereof, RADCHENKO, IEREMENKO, and others, committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about May 6, 2016, RADCHENKO, IEREMENKO, and others, accessed and caused to be accessed the SEC's EDGAR servers, without authorization, from the Romanian IP Address.

b. On or about May 10, 2016, RADCHENKO, IEREMENKO, and others, purchased and caused to be purchased, the Lithuanian Server using a Bitcoin address controlled by RADCHENKO.

c. On or about May 19, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 1 that had been uploaded to EDGAR minutes earlier which, at the time, contained material non-public information.

d. On or about July 22, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 2 that had been uploaded to EDGAR hours earlier which, at the time, contained material non-public information.

e. On or about July 29, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's

EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 3 that had been uploaded to EDGAR minutes earlier which, at the time, contained material non-public information.

f. On or about August 4, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 4 that had been uploaded to EDGAR minutes earlier which, at the time, contained material non-public information.

g. On or about August 8, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 5 that had been uploaded to EDGAR hours earlier which, at the time, contained material non-public information.

h. On or about August 17, 2016, RADCHENKO, IEREMENKO, and others, used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers, without authorization, in order to steal a Test Filing for Public Company 1 that had been uploaded to EDGAR minutes earlier which, at the time, contained material non-public information.

All in violation of Title 18, United States Code, Section 371.

Count Two
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

1. The allegations contained in paragraphs 1 through 3, and 5 through 14 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or about February 2016 through in or about March 2017, in Middlesex County, in the District of New Jersey and elsewhere, the defendants,

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO,

did knowingly and intentionally conspire and agree with each other, and others, to intentionally access computers without authorization, and thereby obtain information from a department and agency of the United States, namely the Securities and Exchange Commission, and from a protected computer for the purpose of commercial advantage and private financial gain, the value of such information being in excess of $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(B), (a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii).

Goal of the Conspiracy

3. It was the goal of the conspiracy for RADCHENKO, IEREMENKO, and others, to gain unlawful access to the computer networks of the SEC for commercial advantage and private financial gain.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and to effect its unlawful objects, RADCHENKO, IEREMENKO, and others, engaged in a number of means and

methods, including those referred to in paragraphs 6 through 13 of Count One, among others.

Overt Acts

5. In furtherance of the conspiracy and to effect the unlawful objects thereof, RADCHENKO, IEREMENKO, and others committed and caused to be committed a number of overt acts, including those referred to in paragraph 14 of Count One, among others.

All in violation of Title 18, United States Code, Section 371.

Count Three
(Conspiracy to Commit Wire Fraud)

1. The allegations contained in paragraphs 1 through 3, and 5 through 14 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or about February 2016 through in or about March 2017, in Middlesex County, in the District of New Jersey and elsewhere, defendants,

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO,

did knowingly and intentionally conspire and agree with each other, CC-1, and others to devise a scheme and artifice to defraud the SEC and the publicly traded companies whose Test Filings they stole (the "Public Companies"), and to obtain money and property, including confidential and economically valuable business information of the Public Companies that constituted material non-public information, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Goal of the Conspiracy

3. It was the goal of the conspiracy for RADCHENKO, IEREMENKO, CC-1, and others, to unlawfully enrich themselves by: (a) hacking into the computer networks of the SEC through a variety of deceptive techniques; (b)

stealing Test Filings containing confidential and economically valuable business information constituting material non-public information; and (c) profiting by selling the material non-public information and trading ahead of its public disclosure.

Manner and Means of the Conspiracy

4. To carry out the conspiracy and to effect its unlawful objects, RADCHENKO, IEREMENKO, and others, engaged in a number of means and methods, including those referred to in paragraphs 6 through 13 of Count One, among others, and those described below.

5. It was part of the conspiracy that the defendants and others deprived the SEC and the Public Companies of their right to control the use of the confidential and economically valuable business information contained in the Test Filings, including the decision of when and how the information should be disclosed to the public.

6. Throughout the course of the conspiracy and in furtherance of their fraudulent scheme, RADCHENKO, IEREMENKO, and others, caused writings, signs, signals, pictures, and sounds to be made and received in interstate and foreign commerce.

All in violation of Title 18, United States Code, Section 1349.

Counts Four through Nine
(Wire Fraud)

1. The allegations contained in paragraphs 1 through 3, and 5 through 14 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From in or about February 2016 through in or about March 2017, in Middlesex County, in the District of New Jersey and elsewhere, defendants,

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO,

did knowingly and intentionally devise a scheme and artifice to defraud, namely, the scheme described in Count Three, and to obtain money and property, including the confidential business information of the Public Companies, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did knowingly transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, and sounds, as set forth below, each constituting a separate count of this Indictment:

Count	Approximate Date	Description
Four	May 19, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 1.

Count	Approximate Date	Description
Five	July 22, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 2.
Six	July 29, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 3.
Seven	August 4, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 4.
Eight	August 8, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 5.
Nine	August 17, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 1.

In violation of Title 18, United States Code, Section 1343.

Counts Ten through Sixteen
(Fraud and Related Activity in Connection with Computers)

1. The allegations contained in paragraphs 1 through 3, and 5 through 14 of Count One of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendants,

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO,

did knowingly and intentionally access and cause to be accessed computers without authorization, and thereby obtain information from a department and agency of the United States, namely the Securities and Exchange Commission, and from a protected computer for the purpose of commercial advantage and private financial gain, the value of such information being in excess of $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B), (a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii), each constituting a separate count of this Indictment:

Count	Approximate Date	Description
Ten	May 6, 2016	Accessed and caused to be accessed the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, from the Romanian IP Address.
Eleven	May 19, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 1.

Count	Approximate Date	Description
Twelve	July 22, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 2.
Thirteen	July 29, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 3.
Fourteen	August 4, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 4.
Fifteen	August 8, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 5.
Sixteen	August 17, 2016	Used and caused to be used the Lithuanian Server to access the SEC's EDGAR servers in Middlesex County, New Jersey, without authorization, in order to access a Test Filing associated with Public Company 1.

In violation of Title 18, United States Code, Sections 1030(a)(2)(B), (a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii), and 2.

FORFEITURE ALLEGATION AS TO COUNTS ONE AND THREE THROUGH NINE

1. As a result of committing the offenses charged in Counts One and Counts Three through Nine of this Indictment, the defendants charged in each respective count shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offense, and all property traceable thereto.

FORFEITURE ALLEGATION AS TO COUNTS TWO AND TEN THROUGH SIXTEEN

2. As a result of committing the offenses charged in Counts Two and Counts Ten through Sixteen of this Indictment, the defendants charged in each respective count shall forfeit to the United States

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts Two and Counts Ten through Sixteen of this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts Two and Counts Ten through Sixteen of this Indictment.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

3. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c) and 18 U.S.C. §§ 982(b) and 1030(i)), to forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A True Bill,

_____
Foreperson

Craig Carpenito

CRAIG CARPENITO
United States Attorney

CASE NUMBER: _____

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

ARTEM RADCHENKO and
OLEKSANDR IEREMENKO

INDICTMENT FOR

18 U.S.C. §§ 371, 1030, 1343, 1349, 2

A True Bill,

_____

Foreperson

CRAIG CARPENITO
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY

DANIEL SHAPIRO, JUSTIN HERRING, AND NICHOLAS GRIPPO, ASSISTANT U.S. ATTORNEYS
LYNN O'CONNOR, SPECIAL ASSISTANT U.S. ATTORNEY
AARASH HAGHIGHAT, CCIPS TRIAL ATTORNEY
NEWARK, NEW JERSEY (973) 353-6087